Amendments to the Specification:

1.) Please replace the abstract with the following rewritten abstract:

A network is provided comprising at least one access point ~~(AP1, AP2)~~ and one access-controlling node ~~(WSN, AS)~~ whereby the identity of the station can be approved by the access controlling node ~~(WSN, AS)~~. The at least one access-controlling node ~~WSN~~ issues at least one Inter-Access Point Protocol ~~IAPP~~ message causing the ~~AP~~ access point with which the station is currently associated to disassociate the given station thereby terminating the access for the given station.

2.) Please replace the paragraph beginning at page 1, line 13, with the following rewritten paragraph:

Wireless LAN (WLAN), and in particular WLAN based on the IEEE 802.11 standard, has in the last few years received tremendous interest. WLANs are used in home and ~~enterprises~~ enterprise environments. WLANs have also become available to WLAN subscribers at public sites, so called hot-spots, e.g. cafes, airports etc. In order to finance these hot spots, the owner of the WLAN infrastructure, such as the service provider, must be able to control access to the WLAN in order to charge customers for its use.

3.) Please replace the paragraph beginning at page 1, line 26, with the following rewritten paragraph:

The most common solution today is that the access control and the collecting of accounting data are performed by the WSN. This solution has been schematically illustrated in FIG. 2. The APs are simply pass-through devices when it comes to access control. Users log in to the system using a HTTP (Hypertext Transfer Protocol) web interface between the UE (User equipment) and WSN. The HTTP traffic between UE and WSN is typically cryptographically protected by e.g. SSL (Secure Socket Layer). In order to verify the credentials received from the UE, the WSN (Wireless Serving Node) typically has a ~~RADIUS~~ Remote Authentication Dial In User Service (RADIUS) client that communicates with an Authentication Server (AS).

4.) Please replace the paragraph beginning at page 2, line 1, with the following rewritten paragraph:

~~These steps shall be briefly described here.~~ In steps 21-27 the well-known steps of the station STA1 authenticating itself and subsequently being accepted for association by the access point AP1 is shown. In step 50 the user of the station opens a web browser and forwards a HTTP Get request 53. The requested web address (URL) does not have to point to the gateway node WSN since the WSN can intercept and redirect the request. The gateway node responds by issuing a HTTP log in page 55. The user then enters his name and password 57 and forwards this information 59 to the gateway node WSN. Upon acceptance the gateway provides a HTTP session window 61, issues a start accounting message to the authentication server AS 63 and opens for traffic to/from the station 65.

5.) Please replace the paragraph beginning at page 3, line 34, with the following rewritten paragraph:

Some AP vendors have implemented [[a]] an IAPP related (non-standardized) functionality: If a layer-2 frame appears on the wired network side of the (previous) AP with the UE's MAC address as the source address, the AP knows that the UE must be associated to some other (subsequent) AP. The previous AP can then remove the UE from its memory and transmit a Disassociation message to the UE.

6.) Please delete the paragraph beginning at page 5, line 6.

~~This object has been accomplished by the subject matter set forth in claim 1.~~

7.) Please delete the paragraph beginning at page 5, line 11.

~~This object has been accomplished by the subject matter of claim 7.~~

8.) Please delete the paragraph beginning at page 5, line 16.

~~This object has been accomplished by the subject matter of claim 9.~~

9.) Please replace the paragraph beginning at page 7, line 20, with the following rewritten paragraph:

AP1 and AP2 respond by issuing IAPP move response messages [[111]] 109 and 113 and at that point the access in the AP's is withdrawn for the using entity STA1 in question. Subsequently, the AP's send Dissociate messages 115 and 117 to station STA1 whereby it is possible for an application running on the station, such as a browser, to positively inform the user that access has been withdrawn, as indicated by the lock out indication in step 119.

10.) Please replace the paragraph beginning at page 8, line 32, with the following rewritten paragraph:

It is noted that since IAPP messages are transported in IP packets, the WSN does not have to reside on the same subnet as the APs. The WSN could send a subnet-directed broadcast 131 to the subnets with the APs of interest. This embodiment has been illustrated in FIG. 9.

11.) Please replace the paragraph beginning at page 9, line 15, with the following rewritten paragraph:

Initially when a RADIUS enabled AP client is powered up on the network, step 83, it issues a RADIUS registration access-request 85 to the WSN or the AS, and the latter node responds with a RADIUS registration access-accept 87 containing means for cryptographically protecting IAPP ADD messages.

* * *